TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 23rd to 29th of April, 2023
Report No.: TZ-CERT/WRHP/2023/17

1. NETWORK ATTACKS

A total of **256,836** attacks have been recorded compared to last week **184,195** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords is as in **table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	116.105.210.32	root	admin
2.	193.105.134.95	admin	123456
3.	116.98.161.120	support	P@ssw0rd
4.	195.3.147.52	ftp	password
5.	171.251.28.138	user	PlcmSplp
6.	54.38.241.159	test	1234qwer
7.	116.98.174.214	guest	1234admin
8.	5.10.250.44	postgres	123123
9.	116.98.172.10	ubuntu	Win1doW$
10.	196.245.250.10	oracle	user

Table1: Top 10 Network attacking IP

Most of the usernames and passwords listed are commonly used, thus its advised review of usernames and password be made to avoid use of the above listed credentials and default ones. Use of password policies is the best practice.

2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded, a total of **787,141** malicious software distributed compared to last week in which was **229,283.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.203.31	Trojan.Gen.NPE	aa13166a6b5409c7b08fa1e5b593e48eb92027ce23efb51f26a33751ecf32a45
2.	41.59.86.254	downloader.linux/medusa	77a2c317ca9d43acc056cf8217a8c838d23af63965b33dc931877360d5919b8d
3.	41.59.211.41	downloader.linux/medusa	36bc49ede8e0f4a54449602ca2bc681f96b14869841a243ddfb7d94fb6f28749

4.	41.59.194.240	downloader.linux/medusa	599060a0d310f4a1b506ac57b519d7d46a53292421be74294f314ae574245fc0
5.	41.59.201.7	trojan.linux/mirai	7443b3707c9db0c5ed6c8acef9d60128932c8e3f3f7bdeed1d2bba4598013f81
6.	41.59.201.132	trojan.linux/xorddos	d42fef60e13ef1c7ccb1039044bbf307c5d4417a7abf0b271956cef6e2d593be
7.	85.208.107.26	trojan.linux	e1bc6d3db47deb43a8c6c1a3c9d9d1ba7e336d1e6e5f63843b8450c8029bc3af
8.	58.57.4.26	Trojan.Linux.Generic.246192	6e09788f61ff2ae15d6d0e2a4a7e66f9dcd0db92b26a90f06be8390c791789ac
9.	36.79.87.146	Trojan.Win32.Eb.dqb	746a154e5586816d0c3c63a84a7974135135b0b6b54f452018a20ad43fe11835
10.	154.178.233.66	rojan.linux/xorddos	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,961** web attacks compared to last week which was **3,936.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 23rd to 29th of April, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	122.168.198.123	/
2.	92.234.178.185	/get
3.	45.58.56.46	/users/sign_in
4.	193.32.162.159	/adcr.nhn
5.	45.141.215.105	/.env
6.	190.104.10.239	/boaform/admin/formLogin

7.	88.227.149.195	/favicon.ico
8.	173.249.46.215	/recordings/
9.	152.89.196.222	/manager/html
10.	109.237.96.251	/robots.txt

Table3: Top 10 web attacking IP

4. RECOMMENDATIONS

The Honeypot sensors have recorded IP addresses with most common malware used in the world today. Monitoring of the listed IP address is advised and further to: -

4.1 Note that most of malicious IP addresses captured are also listed as malicious IP addresses in other sources that are also observing security attacks; thus, security measures should be considered to counter act, including monitoring of the IPs in networks. Most likely the same resources might be used for further attacks.

4.2 Discourage usage of listed login resources (usernames and passwords) and consider deploying mechanisms to monitor login attempts.

4.3 Thoroughly check for suspicious files of hashes listed in **Table 2**.

4.4 Deploy Intrusion Detection System (IDS) and configure to flag detection of attacks associated with list of resources provided especially the IP addresses and the web requests.